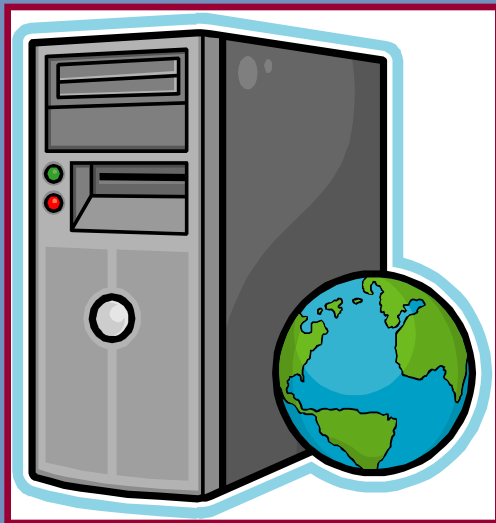


# When Federal Employees Abuse Technology: From Policy to Discipline



Barbara I. Haga  
Federal HR Services, Inc.

DELRS Phoenix, AZ  
April 2011

# Technology in the Workplace

- Improvements in technology and the way we work lead to new issues for managers, unions, and HR/Legal
- Technology is everywhere – as are the workplace issues associated with it



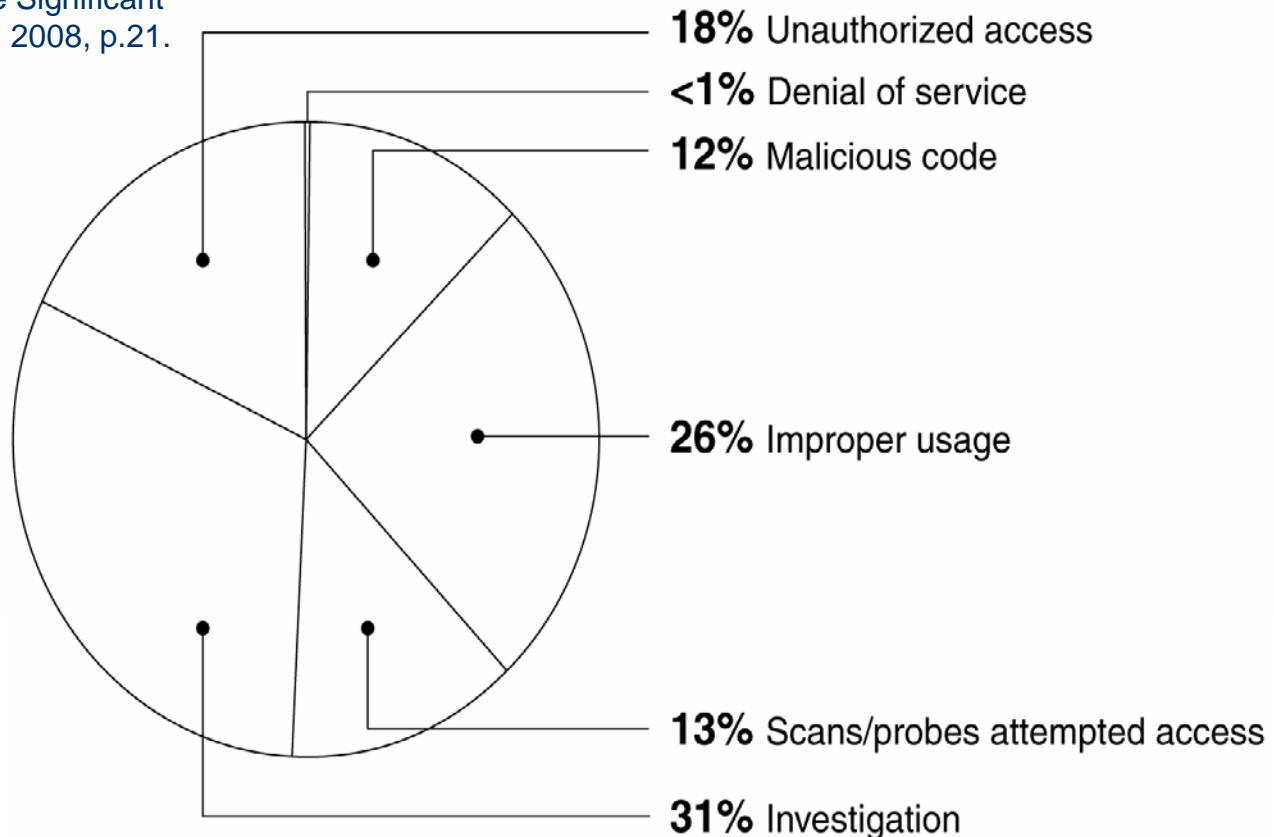
# Recent Technology-related Issues

- Use of Internet/e-mail
  - Potential Government Shutdown
    - Question: Would agencies be required to turn off outside access to computer systems to avoid accepting “free” labor during furlough?
- Porn “scandals”
  - SEC, NSF, Gettysburg
- Cell phones
  - EO 13513, “Federal Leadership on Reducing Text Messaging While Driving”
  - Evidence – picture of an employee sleeping on duty (CBP Arbitration, Blaine, WA (2009))
- Telework Program
  - Snowmageddon - Blizzard of 2010



# GAO Report on Information Security

From GAO -08-496T, Information Security:  
Although Progress Reported, Federal  
Agencies Need to Resolve Significant  
Deficiencies, February 14, 2008, p.21.



Source: GAO analysis of US-CERT data.

# Today's Topics



- Misconduct
- FLRA/FSIP and technology-related matters
- Labor agreement language
- Policies covering use of technology

# Misconduct

- Primarily falls in three categories

- Accessing inappropriate material (sexually explicit, pornographic, obscene)



- Using government equipment for activities that are not “inappropriate” but qualify as misconduct



- Not protecting information to which the employee is provided access in the course of his/her employment or unauthorized use of information



# Types of Misconduct – Sexually Explicit Material

- Group One – arrested and taken away
  - Possession of child pornography is a crime (18 USC Chapter 110)
  - Bross v. Commerce (2004) (Fed. Cir.) – convicted and sentenced to three years probation on conditions that included regular counseling, the possibility of searches of work or home computers, and notification of his employer of the conditions/ restrictions on his computer use



# Indefinite Suspension

## ■ DoD investigation

- Operation Flicker was a nationwide investigation that identified over 5,000 individuals who subscribed to certain child pornography websites (Google)
- Identified DoD employees and contractors who used .mil addresses in accessing websites
- Oswald, a Telecommunications Specialist, GS-9, at NAS Pt Mugu CA was identified and arrested 8/6/2008
- Indefinitely suspended effective 12/22/2008 based on criminal charges
- Ultimately sentenced to 16 months incarceration, in addition to registration with the National Sex Offender Registry
- Removed from his employment on 5/16/2009 (Oswald (2009) 2 decisions)



# Types of Misconduct – Sexually Explicit Material II

- Group Two – do not break any laws but violate policy
  - Merritt v. Air Force (2006) (ID) – repeatedly visited pornographic websites, received numerous sexually explicit e-mails which he opened
  - Hollenbeck v. Air Force (2004) (ID) - engaged in inappropriate communications, stored sexually offensive material, sent and received sexually related e-mails
  - Reinhardt v. Air Force (2005) (ID) – willfully used agency computers to visit sexually explicit websites and download images and motion pictures
  - USDA and AFGE 3354 (2006) Arbitration – GS-7 Budget Technician Williams averaged two hours per day surfing the Internet on subjects which interested him, including pornography



# Charges related to sexually explicit material

## ■ Criminal

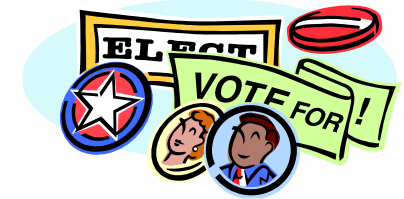
- Illegally downloading child pornography from the Internet to government computer (Bross)
- Commission of a crime for which a sentence of imprisonment may be imposed (Oswald)

## ■ Sexually Explicit material

- Accessing sexually oriented websites (Merritt)
- Storing material with sexually graphic pictures on computer (Hollenbeck, Merritt)
- Misuse of government computers and wanton disregard of directives (Hollenbeck)
- Violating agency policy (USDA/AFGE Williams)
- Unauthorized use of agency computer system to view and forward sexually explicit material to another agency employee and to persons outside the agency (Schoeny v. VA (2003) (ID))

# Personal Use

- Using government resources for unofficial activities:



- Biniak v. SSA (2002) – GS-12 Computer Specialist operated a financial planning business
  - Calls recorded to clients, files related to business found on his computer, used a phone line to connect to an internet service provider in spite of being denied a modem, loaded Turbo Tax and Quicken on his computer
- Eisinger v. MSPB (2007) (Fed. Cir. unpublished)
  - Staff Attorney with SBA removed for Hatch Act violation
  - Admitted that between 2001 and 2004 he performed activities directed toward the success of the Green Party – for a “significant amount” of time
  - Used government e-mail account to send numerous messages, held telephone conversations, drafted documents

# More Personal Use

- Using government resources for unofficial activities:
  - Grossman v AF (2010) (ID)
  - GG-13 Command Post Manager at Los Angeles AFB downgraded to 12
  - Charges related 1) using government computer, e-mail, and Internet and other resources to facilitate his private law practice and 2) ethics violation of free legal service to his supervisor in supervisor's divorce
  - Admitted he used the resources in representing individuals as a private attorney
    - Said he was getting experience so he could get a JAG position
    - Didn't abuse resources "excessively"



# “Wasting Time”

- Employees engaged in computer activities unrelated to their jobs are not working
- Famous quotes:
  - She planned her wedding at work, including sending and receiving e-mails and visiting wedding Internet sites. Stated she was a multi-tasker and able to complete her job duties notwithstanding the inappropriate computer activity (Quirarte-Ortiz v. EPA, 2007 (ID))
  - He was having an adulterous affair with student hire. Stated messages were short and he was able to send her as many as 89 e-mails in 5-10 minutes and it wouldn't interfere with his work (Hollenbeck)
- Another time waster
  - HR Assistant spent roughly 84 hours of work time in several periods between 4/21 through 6/8/2009 on non-work related websites
  - Prior counseling and one-day suspension in 2008 for same issue
  - Acknowledged misconduct and apologized
  - Stated she didn't intend to harm the agency; could have performed additional work such as assisting the other employees instead of spending time on Internet (Rose v. VA (2009 (ID))



# Wasting More Time

- Kelly v. Agriculture (2007) (Fed. Cir. remand)
  - Resources Management Specialist removed for a variety of attendance issues also charged with improper conduct – sharing jokes and watching “Oprah” on her computer
- Reynolds v. Labor (2003) (ID)
  - Fiscal Technician GS-6 retired in lieu of being removed
    - 69 e-mail folders on computer – 63 were personal
    - In 18 month period investigated employee had hits on 7600 different websites
    - Sent sexually explicit e-mail messages and attachments
- Rush v. Air Force (1996)
  - GS-7 Supply Technician removed for misuse
  - Multiple charges related to excessive use of government computer and printer for personal reasons; did not stop even after repeated warnings
  - Action sustained on PFR even when only formal discipline for like offense overturned by an arbitrator



# King of Time Wasters

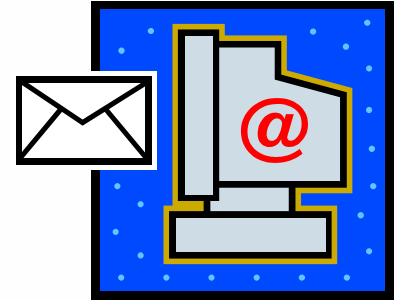
- Parvin v. Army (2007) (ID)
  - WG-8 Toxic Test Equipment Inspector suspended for 20 days for –
    - Installing a wireless arm system on a Federal installation to alert him to personnel approaching the work area
    - Using his personal computer (his personal property) during duty hours to work on personal projects
    - Misuse of government property (related to the way he installed the alarm)
  - Parvin said that it was a practice for employees to be on “paid break” time and engage in personal activities whenever their assignments were completed



# “Wasting Time” Charges

## ■ Similar charges

- Misuse of government computer (Reynolds, Quirarte-Ortiz, Rush)
- Improper/inappropriate conduct (Kelly & Rose)
- Failure to follow instructions (Reynolds)



## ■ Board's view:

- Misuse – Hoyle v. Energy (2004) (ID)
  - Agency must prove only that appellant used property belonging to the government and use was not authorized
  - No requirement to prove employee had notice or acted with intent
  - Lack of notice is considered in assessing the reasonableness of the penalty – Douglas
- Not working when on duty time (Quirarte-Ortiz)
  - “There is a deleterious relationship between the appellant’s use of government equipment to conduct extensive personal business during duty hours and the efficiency of the service. The appellant was expected to conduct government business during duty hours.”

# Unauthorized use of information

- Accessing system for non job-related purposes
  - Schoeny - GS-12 Computer Specialist (also a union official) charged with:
    - Accessing the e-mail accounts of personnel without authorization and disclosing information to the union
    - Auditing his supervisor's access to an agency automated system without permission to do the audit
  - Social Security Administration
    - Agency policy on discipline "Sanctions for Unauthorized System Access Violations"
    - Classifies types of violations and provides recommended penalties



# Social Security Access Violations

- Quoted in 2005 arbitration decision
  - Category I - Unauthorized Access without Disclosure
    - First offense – Minimum 2-day suspension
    - Second offense – Minimum 14-day suspension
    - Third offense – Removal
  - Category IIA –employee improperly accesses a record and discloses info to person entitled to receive it (same penalties as category I)
  - Category IIB – employee improperly accesses a record and discloses info to person not entitled to receive it
    - First offense – Minimum 14-day suspension
    - Second offense – Removal
  - Category III – Unauthorized Access for Personal Gain or with Malicious Intent
    - First offense - Removal



# Love Hurts (IRS Access Violation)



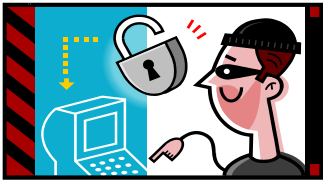
- IRS Clerk accessed records on 7 private individuals
- One was a woman she believed was involved with her boyfriend and others were people with whom the woman was involved
- Charged criminally – indefinite suspension proposed by IRS (but nearly four years after learned of misconduct)
- Pled guilty in court – probation for one year, 100 hours of community service, \$500 fine
- Indefinite suspension overturned but agency subsequently issued a proposal to remove Wu v. Treasury, (2010) (ID)

# Unauthorized disclosures

- Unauthorized disclosure of personally identifiable information
  - privacyrights.org tracks disclosures across country
  - As of January 4, 2011
    - 2,219 data breaches made public since 2005
    - 511,134,665 records breached
- Government record breaches
  - Department of Interior - CD containing personally identifiable information for about 7,500 federal employees reported lost by Department's shared services center in May 2010
  - TSA - Office of Human Capital lost external hard drive which contained 100,000 archived employment records including SSN's, DOB's, bank account and routing info
    - Unsuccessfully sued by AFGE for violation of Privacy Act 5/07 – (AFGE, et al v. Kip Hawley and TSA)

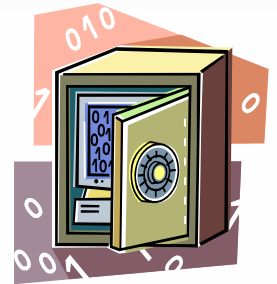
# Not following rules for protecting info

- Veterans Administration May 2006
  - Analyst took data files home without authorization
  - Employee's home was broken into – laptop and hard drive stolen
  - Info in the files included
    - Names and DOB's for 26.5 million veterans and spouses
    - SSN's for 19.6 million veterans
    - Info on as many as 1.1 million active duty personnel
  - Laptop was recovered and forensic analysts concluded unlikely that information was compromised
- No disciplinary action identified through review of MSPB decisions



# More failures

- Other failures identified:
  - Not following established security procedures and verifying that established procedures are followed
  - Not implementing property accountability procedures and enforcing them
  - Not ensuring that computer systems have the most current fixes
- Performance issues for those responsible for implementing/enforcing policies and disciplinary issues for those who fail to follow requirements



# Employee Defenses

- “I didn’t understand that there was a policy against it”
  - In misuse cases, agency not required to show employee had notice not to misuse - need only show that the property belonged to the agency and use was not authorized
  - Notification not to engage illegal activity not necessary - but notification of restrictions on use of computers for other types of activities that qualify misconduct is important in Douglas to show employee on notice
  - Most of cited cases had ample evidence of employee notification through directives and training, and some personal notifications, warnings, and prior discipline



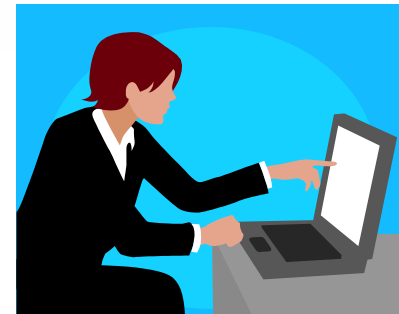
# Employee Defenses II

- Misuse discovered through “illegal” means
  - Winters v. Navy (2007) (Fed. Cir. non-precedent.)
    - Set up a website from work computer with over 250 pages of material about his work situation posted
    - Web page publicly identified him as a government employee, identified his duties and work location, and expressed his extreme dissatisfaction with his superiors
    - Misuse discovered in preparing response to unrelated FOIA request
    - “FOIA standards are in place to protect agency from taking unreasonable measures to respond to a request. They do not protect agency employees from the agency gathering information in response to a FOIA request.”



# Defense II – expectation of privacy

- GSA Model Policy on Personal Use of Government Office Equipment (Paragraph 4F)
  - Executive Branch employees do not have a right, nor should they have an expectation, of privacy while using any Government office equipment, at any time, including accessing the Internet, using E-mail (sic).
  - To the extent that employees wish their private activities remain private, they should avoid using an Agency or department's office equipment such as their computer, the Internet, or E-mail.
  - By using Government office equipment, executive branch employees imply their consent to disclosing the contents of any files or information maintained or pass-through (sic) Government office equipment



# Defense II – more on privacy

- Supreme Court ruling 6/2010 on search of text messages on employer-provided cell phone
  - Quon was a law enforcement officer who exceeded allotted amount of text messages
  - Chief requested a review of messages to see if the limit on the messages was reasonable
  - In the course of review determined that some of his messages were personal and some sexually explicit – Quon was disciplined for violating policy
  - Search found to be reasonable by Supreme Court
  - “As a law enforcement officer, [Quon] would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications.” (City of Ontario v Quon)



DELRS April 2014

# Employee Defenses III

- “I have a sexual addiction”



- Sexual behavior disorders are not protected under the Rehabilitation Act
- 1992 amendments to the Rehabilitation Act removed transvestitism, transsexualism, pedophilia, exhibitionism, voyeurism, gender identity disorders not resulting from physical impairments, and other *sexual behavior disorders* from definition of “individual with a disability”
- 2008 ADA amendments did not change exclusion
- Browder v. Navy (1999) (Fed. Cir.)

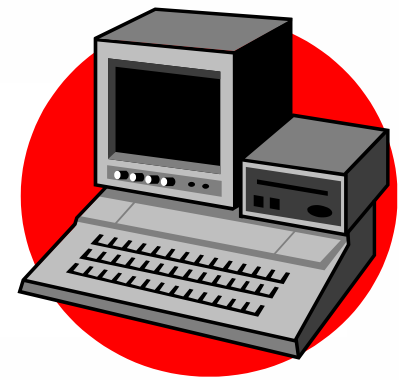
# Sexual Behavior Disorders and Retirement

- Combs v. OPM (2005) (ID)
  - Army employee arrested while on home leave in the United States for trafficking in child pornography
  - Resigned from his position two months later
  - Filed for disability retirement six months later based on sexual perversion and adjustment reactions which began at the time of the arrest
  - Medical documentation indicated that he was depressed
  - No job deficiencies noted other than minor attendance issues
  - Except for arrest he would have remained in his Museum Curator position
  - Did not meet burden of showing that while employed he became disabled because of a medical condition resulting in a severe deficiency in performance, conduct, or attendance

# Employee Defenses IV

- “I was frustrated”

- Patrol Agent in Charge disciplined for several charges – two related to language and use of a government vehicle
- Third charge was “inappropriate display of a firearm”
- Admitted to removing his loaded gun from its holster and pointing it at his computer and telephone
- Did it when the phone was ringing a lot or his computer was having problems (Perez v Homeland Security, (2009))



# Position occupied and Douglas

## ■ Computer-related positions

- Bross - GS-13 Computer Specialist arrested for downloading child pornography
- Hollenbeck – Information Technology Specialist (Security/Network Services) – utilized knowledge of system to bypass system protocols to engage in inappropriate communications; stored sexually offensive material; sent and received sexually related e-mails . . . .
- Quirarte-Ortiz – GS-12 Information Technology Specialist – repeatedly used government computer during work hours to plan her wedding and stored material related to a commercial business
- Merritt – GS-11 Equipment Specialist (Electronic) – used unauthorized freeware to bypass agency network security

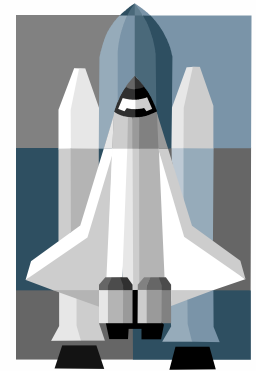


# Supervisory Positions

- Personally involved in inappropriate activities
  - Coons v. Treasury (2005) (ID) – GM-15 Program Manager accessed sexually explicit sites – more than a few accesses daily and occurred over a significant number of months
    - Worked in the Collections Division-highly sensitive area under intense scrutiny by Congress and also lied about wrongdoing
  - Martin v. Transportation (2006) – Supervisory Aviation Safety Inspector FV-14 used computer to access sexually explicit material
    - Regular extended non-work-related Internet searches
    - 71 pictures on hard drive of nude or partially nude men and women, some depicting sexual acts

# More on Supervisory Positions

- Failed to take action to deal with computer misuse by subordinates
  - Tatum v. NASA (1998) (ID) - GS-15  
Supervisory Aerospace Engineer did not take action to ensure subordinate stopped downloading sexually explicit material
  - That employee ultimately criminally charged
  - Downgrade mitigated to 60-day suspension



# Positions of Trust

- Security Guard – Anderson v. Army (2005) (ID)

Security Guard accessed an unsecured computer and sent out e-mails to four addressees to let superiors know that an employee failed to follow shut down procedures



- Security Clearance – McDaniel v. Navy (2003) (ID)

Engineer with Top Secret security clearance downloaded and sent out voluminous amount of sexually explicit material, some of which was violent in nature



- Agency representative - Von Muller v. Energy (2006)

GS-14 Economic Development Account Executive used computer to send sexually explicit material both inside and outside the agency



# Accommodation

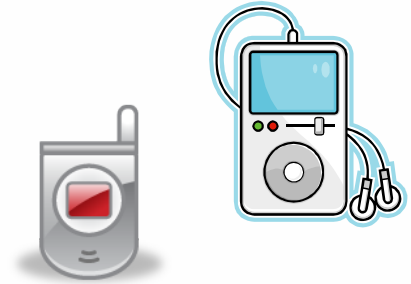


- McKelvey v. Army, (2009 U. S. District Court Decision)
  - Disabled vet needed computer equipment
  - Supervisor said there was no money for that kind of “sh\_\_”
- Computer Electronic Accommodation Program
  - Since 2000 open to all Federal agencies
  - Provides assistive technology, devices, and services at no charge to agency or employee



# Labor Relations considerations

- Personal use of cell phones, MP3 players, and/or computers has not been an issue in many negotiability/ULP/impasse cases
- Cell Phones
  - Homeland Security and NTEU (FSIP (2004))
    - Issue: Border Patrol employees in field being accessible by cell phone
    - Agency banned privately owned pagers/cell phones from the workplace after an immigration inspector used a personal cell phone to try to allow drug smugglers to enter US without inspection
    - Union proposed that there be one manned number to receive emergency calls at any location where cell phones were prohibited
    - Agency argued that it interfered with right to determine method and means of performing working and right to determine internal security practices
    - FSIP ruled that the benefits to employees outweighed the costs and ordered adoption of the Union's proposal



# Additional Labor Relations issues

- Cell phones and Border Guards (cont'd)
  - Subsequent Arbitration Review (FLRA 2010)
    - Agency refused to implement impasse decision
    - FLRA found award contrary to law ordered implementation (installation of phone lines) in 30 days
- Cell phones - Negotiability
  - Air Force and AFGE (FSIP 2005)
    - Base commander issued instruction prohibiting cell phones while driving on base and in any aircraft maintenance areas
    - Union wanted to bargain substance; agency refused – I&I only.
    - Sent to FLRA for negotiability determination

# More on Negotiability



- ATC's prohibited from having cell phones and similar devices
  - Union wanted non-audible use of pagers and cell phones
  - Agency argued that could interfere with equipment and presented a distraction
- FLRA found outside duty to bargain and not an appropriate arrangement (NATCA v FAA (2009))

# Telework and Internet connections

- ATFE and NTEU (FSIP 2006)
  - Union proposed that the agency pay half of the cost of high speed internet connections for teleworkers
  - Agency said that high speed connect would only be needed infrequently – employees could come into office; administrative burden to see that employees were obtaining cheapest available serve; *might* be unlawful under GSA guidance
  - Union said teleworkers should be as productive at home as at work; Cost \$225,000 annually.
  - FSIP found cost too high, no offset of costs through cutting office space, no real hindrance of work performance



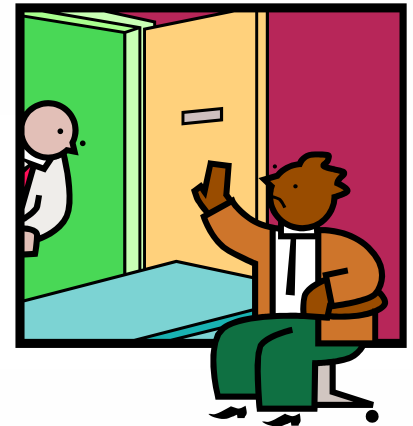
# Computer use/information security policies

- Comply with GSA Model Policy on Personal Use of Government Office Equipment published by the Federal CIO council and OMB Circular A-130 on Management of Federal Information Resources
- Explain clearly what is and what is not prohibited
- Customize to cover specific situations in your agency – telework arrangements, types of information handled, work while on travel, fixes for past problems, etc.
- Take advantage of work done in other organizations – look at their policies/cases/agreements and use what it applicable
- Consider revising table of penalties to add detail on technology-related and information security offenses



# Telework Programs

- Authorizing work at alternate locations adds new issues relating to misuse of government computers and protection of information
  - Telework arrangements may involve providing government equipment
  - Protection of data while in employee's custody is a tremendous concern
- GSA Guidance
  - Telework Overview, Telework Library
  - Link in case listing



# Contract Language

## ■ DCAA Central Region and AFGE Local 3529

### ■ Article 38 Telework

#### ■ Section 38:04 –



- 10 Protection of government/agency/ contractor records – no classified documents may be taken out
- 17 – Employee must have a safe and adequate place to work offsite that provides the necessary level of security and protection for Government property
- 19 – Telework arrangements should be imperceptible to customers and outside sources
- 26 – Employer provided laptop and software to be used only for official business except limited personal usage under normal computer use policy
- Section 38:07 Tasks and Work Activities – list certain tasks that must be performed at traditional worksite and what can be done at the alternate site

# Contract Language – DCAA/AFGE

- Article 47: Use of Government Office Equipment
  - 47:02 - Authorized uses (subject to typical restrictions): preparation of a personal letter, or other document, or spreadsheet, access to the Internet for personal use, sending/receiving personal e-mail
  - 47:03 - Misuse includes: installation of personal internet account on a government computer, installation of personally owned software or hardware, freeware/shareware, connection to data stream sites, creation/copying/transmission or retransmission of chain letters or unauthorized mass mailing, engaging in any outside fund raising activity, posting agency information to external newsgroups, bulletin boards or other public forums without authority
  - 47:05 – Personal use includes assisting relatives, friends, or other persons in any such activities
  - 47:09 – Procedures for removal of personally owned software or hardware, freeware or shareware



# Contract Language Examples

- Naval Air Warfare Center and AFGE Local 2113
  - Authorized uses:
    - Access and use of Internet for professional development purposes, such as reading magazine articles, research, etc.
    - Access and use of e-mail in support of non-Federal and not-for profit work-related professional organizations
  - Electronic Correspondence Responsibilities
    - Employees who have incidental access to electronic mail will not view others' electronic mail for their own personal interest. Content of mail viewed for official reasons will be treated with reasonable confidentiality except for inappropriate or unauthorized use of Internet

# Consequences of Contract Language

- Arbitration review - SSA and AFGGE Local 1760
  - Contract guaranteed Union limited access to e-mail
    - Local President retired but continued to serve as President
    - Agency then denied access to e-mail and official time tracking system
    - Union grieved. Agency argued internal security and violation of policies. Union said was required to fulfill President's role
    - Arbitrator noted that language was not clear. Also noted that contract required notification of changes by electronic means, that President had had access for years without incident, contract required Union to conform to Agency requirements for security. Found contract did say that any employee leaving would lose access
    - Arbitrator found agency violated agreement and FLRA upheld award

# Agency Directives

- **FDIC – Policy on Use of Personal Digital Assistants (PDA's)**
  - Provides guidelines for personally owned PDA's used for official purposes and government provided PDA's
  - Subparagraph 7b – Connecting personal device to FDIC workstation
  - Sub paragraph 7d – Corporate inspection provides for
    - Unannounced inspections of FDIC systems and data
    - “A personally owned PDA is considered subject to inspection if it has been used for FDIC business-related purposes or if at any time it has been electronically linked to an FDIC system”
- **HHS Policy on Personal Use**
  - Paragraph 4.4 - prohibited activities
    - Using another person's digital authentication
    - Sending anonymous messages
    - Avoiding established security procedures



# Cell phones, iPods, etc.

- Devices now have additional capabilities
  - Cameras
  - Ability to upload and download files
- Policies need to be amended to explain conditions for appropriate use
- Reasonable use policies for cell phones and PDA's, Blackberries, MP3's, and digital readers
- Culture change
  - CBA between Puget Sound Naval Shipyard and Intermediate Maintenance Facility and IFPTE Local 12
  - Ground rules:
    - “Both sides shall exhibit professional meeting courtesies, such as turning off cell phone and pager ringers.”



# Blogs and Wikis

- Blogs (web+blog) are sites which allow users to post information on topics of interest
- A wiki is software that allow creation of collaborative websites
- Blogs and wikis allow anyone with access to submit information and on wikis anyone can edit the information
- Blogs are being used in Federal agencies to enhance communication
  - In FY 07 Performance and Accountability Report EEOC stated that a blog had been created in the Office of Communications and Legislative Affairs to “ensure a free flow of information to staff”
- Blogs about agencies and individuals’ particular situations also exist:
  - Dead Men Working: <http://deadmenworking.blogspot.com/> - a “blog created by a group of high-level career Foreign Service Officers whose careers have been damaged or ended by suspension or revocation of our security clearances”



# Postings by employees and observers

- More blogs about Federal employment
  - Government Accountability is a Citizen's Responsibility: <http://civilservicechange.org/>
  - Tag lines:
    - Because Democracy is Not Free — we all have to work at it
    - Everyday Citizens addressing Merit in Government
- Watch sites
  - National Park Watch: <http://nps-reform.blogspot.com/>
  - NASA Watch: <http://www.nasawatch.com/>



# Blogs and discipline

- An IBM discrimination suit contained this footnote:
  - O asserts that two of his fellow employees, SS and TP also developed anxiety symptoms due to the way the supervisor treated them. At oral argument, IBM challenged this assertion and proffered that TP voluntarily left the company and SS was *terminated for saying unflattering things about an IBM client in a blog posting.*
- Murray v. Commerce (2007) (ID)
  - GS-12 Meteorologist charged with misuse of government computer
    - Specifications included numerous instances of use of the computer to access a phone sex enterprise and blog and a fetish blog among other sexually related infractions including sending e-mail, shopping for inappropriate items online



# Hatch Act Guidance

- OSC guidance on political activity:
  - Employees are free to express their political opinions on blogs so long as they do it off duty
  - Employees must not identify themselves in their official capacity when they post their opinions
  - Blogging for or against a political party or candidate is prohibited when an employee is on duty, in a federal building or government vehicle, or via remote access to the agency's computer network
  - Federal employees must never solicit campaign contributions. Even a link on a blog page that says "contribute" next to the comment text box is a problem
  - Reading a received political e-mail is not a violation, but if the employee prints it out/distributes it/forwards it while on agency property or on duty or during work hours or through an agency system, it is a violation

Cyberfeds article 02/22/2008

"Update training to avoid technical Hatch Act violations"

# Hatch Act Guidance

- OSC guidance on political activity:
  - Hatch Act FAQ's
    - Subheading “E-mail and Blogging as Political Activity”
  - Ana Galindo-Marrone, Chief Hatch Act Unit, shared reminders during FDR last year
    - Do not include links to political content on official agency Web sites or Facebook pages
    - Avoid linking to a union newsletter if the union endorses a partisan candidate
    - Avoid President Obama's Organizing for America website as it is part of the Democratic National Committee
    - Federal employees can include names, official titles, organizations and political affiliations in Facebook profiles but cannot enter political comments or, for less restricted employees, place links to political organizations or candidates while in a federal building or on official duty.

# Tales of Two Supporters



- OSC v Sewell, (2010)

- VA employee used sent/forwarded over 30 e-mails in support of McCain/against Obama to VA employees and outside individuals
- Log in for computer reminded employees of restrictions
- Messages identified her name and position
- Penalty was removal

- OSC v Ware, (2010)

- Bureau of Engraving and Printing employee was a COTR
- Invited 16 people to a fundraiser for Obama by e-mail
- Sent an e-mail specifically soliciting contributions for the Obama campaign and additional political e-mails to agency employees and contractors
- Should have known of restrictions through written communication and annual Ethics training
- Penalty was removal

# Questions? More info?

Barbara Haga  
Federal HR Services, Inc.  
[bhaga@fedhrservices.com](mailto:bhaga@fedhrservices.com)  
[www.fedhrservices.com](http://www.fedhrservices.com)  
(757) 814-5764